-2

1- رنگ های بسته هایی ک دریافت و ارسال میشوند

نمایش بسته های مختلف به رنگ های مختلف به این دلیل است که کاربر بتواند با یک نگاه کوتاه سریع بفهمد هر بسته که ارسال و دریافت میشود چه نوع بسته ای است. برای مثال به صورت پیشفرض رنگ بنفش کم رنگ به معنای بسته های"TCP" ، رنگ آبی روشن به معنای بسته های "UDP" و رنگ سیاه به معنای بسته هایی است که با ارور مواجه شده اند

2-فیلتر کردن بسته ها

اگر به دنبال چیز خاصی در بین بسته ها میگردید، یعنی اگر برای مثال میخواهید که ترافیکی را که یک نرم افزار حین باز شودن و کار کردن ارسال میکند را مشاهده کنید، راه ساده این است که تمامی دیگر نرم افزار هایی را که از اینترنت استفاده میکنند را ببندید. اما با انجام این کار باز هم ترافیک زیادی در سیستم رد و بدل میشود. اینجاست که وایرشارک و قابلیت فیلتر کردن به کمک شما میایند.

آسان ترین راه برای اعمال یک فیلتر در نرم افزار وایرشارک این است که در آن نوشته "Apply a Filter" فیلتر مورد نظر را در کادری که عبارت شده است تایپ کنید و سپس اینتر بزنید

برای مثال میتوانید عبارت "DNS" را در این کادر وارد کنید و اینتر بزنید تا تنها بسته های DNS را مشاهده کنید

3-تجزیه تحلیل بسته ها

به منظور تجزیه و تحلیل هر بسته بر روی آن کلیک کنید تا هایلایت شود. سپس اطلاعات کاملی راجع به آن در پایین نرم افزار ظاهر خواهند شد

-1
در جزئیات هر بسته، به دنبال بخش " "Transmission Control Protocol (TCP) میگردیم.

در این بخش، می‌توانید پرچم‌های مختلف مربوط به بسته را مشاهده کنید.

معمولاً پرچم‌ها با حروف اختصاری مانند "F" برای FIN، "P" برای PUSH، "U" برای URGENT و "R" برای RESET نمایش داده می‌شوند.

و از اون قسمت بالا فیلتر بندی میکنیم و تک تک پکت هارو نگاه میکنیم ک کدوم فلگ دارد.